We claim:

1. A method for registering two network devices with each other, comprising the steps of:

launching a registration process at said two network devices with a pair of registration triggers supported on said two network devices within a predetermined time interval of one another;

transmitting registration information between said two network devices;

generating a secret at at least one of said two network devices, thereby providing an authenticated communications capability between said two network devices; and

communicating an acknowledgement between said two network devices assuring that the secret is shared between said two network devices.

2. The method of claim 1, further comprising the steps of:

monitoring said registration process for registration communications emitting from a third device;

completing said registration process if no said registration communications emitting from a third device is detected; and

not completing said registration process if registration communications from a third device are detected.

3. The method of claim 1, further including a step of generating a pseudonym designating at least one of said two network devices.

4. The method of claim 1, wherein said registration information does not include a plain-text identity of at least one of said two network devices, thereby making said registration process at least partially hidden.

5. The method of claim 1, wherein registration information includes PIN number information.

6. A system capable of securely registering a device, comprising:

a server supporting a first part of a registration process;

a network device supporting a second part of a registration process;

a communications link coupling said server to said network device;

a pair of registration triggers, said server and said network device each supporting one of said pair of registration triggers, wherein activation of said pair of registration triggers within a predetermined time interval launches said first and second parts of the registration processes, which then communicate with each other through said communications link;

a set of registration data exchanged between said server and said network device over said communications link after the launching of said first and second parts of the registration process;

a cryptographic secret formed at at least one of said server and said network device and shared between said server and said network device, thereby facilitating authentic communications between said server and said network device; and

a database that stores said registration data and said cryptographic secret.

7. The system of claim 6, further comprising a monitoring system that detects a registration signal that might emanate from a third device, whereby detection of said registration signal from said third device prevents registration of said network device as part of said registration process.

8. The system of claim 6, wherein registration of said network device includes the use of a PIN number.

9. The system of claim 6, further including a step of generating a pseudonym for at least one of said server and said network device.

10. The system of claim 6, wherein said registration data for at least one of said server and said network device does not include a plain-text device identifier, thereby making said registration process at least partially hidden.

11. A server that can register a network device, comprising:

a database capable of storing a set of registration information, a set of address information, and a cryptographic secret;

a registration process including communications for registering a network device;

a cryptographic generator that receives cryptographic information, enabling authenticable communications between said server and said network device;

a processor supported on said server; and

a registration trigger coupled to said processor, whereby activating said registration trigger within a predetermined time interval of an activation of a remote registration trigger activates said registration process.

12. The server of claim 11, further comprising a monitoring system that detects registration communications from a third device, wherein detection of said third-device registration communications causes said registration process not to register the network device.

13. The server of claim 11, wherein said set of stored registration information includes at least one pseudonym for a device.

14. The server of claim 11, wherein said registration process is at least partially hidden and does not include an exchange of a plain-text identifier for at least one of said server and said network device.

15. The server of claim 11, wherein said registration process includes use of PIN number information.

16. A network device capable of registering with a server, comprising:

a storage system storing registration information and address information;

a registration process including communications for registering said network device with a server;

a cryptographic system that receives cryptographic information, thereby enabling authentic communications between said server and said network device;

a processor supported on said network device; and

a registration trigger coupled to said processor, whereby activating said registration trigger within a predetermined time interval of an activation of a registration trigger on another device activates said registration process.

17. The network device of claim 16, further comprising a monitoring capability that detects registration communications from a third device, wherein detection of said third-device registration communications causes said registration process not to register the network device.

18. The network device of claim 16, wherein said registration process does not include an exchange of a plain-text device identifier for the device.

19. The network device of claim 16, wherein said registration process includes use of PIN number information.

20. The network device of claim 16, wherein said stored registration information includes a pseudonym for a device.

21. A sequence of messages, comprising:

a network device message communicated in response to an activation of a first registration trigger;

a server message communicated within a predetermined time interval of the communication of said network device startup message in response to an activation of a second registration trigger; and

at least one acknowledgement message communicated on said network and assuring knowledge of a shared secret.

22. The sequence of messages of claim 21, wherein said message sequence includes PIN number information of the network device.

23. The sequence of messages of claim 21, wherein said message sequence includes PIN number information of the server.

24. The sequence of messages of claim 21, wherein said network device registration message does not include a plain-text device identifier for the network device.

25. The sequence of messages of claim 21, wherein said server registration message does not include a plain-text device identifier for the server.

26. A method for establishing a registration between a pair of network devices, comprising the steps of:

exchanging initial messages that are substantially simultaneously broadcast on a network between a first device and a second device, each message initiated in response to a local trigger;

broadcasting a first set of identity information from said first device;

broadcasting a second set of identity information from said second device; and

generating a key at said first device, thereby providing an authenticable communications capability between said first device and said second device.

27. The process of claim 26, further comprising the steps of:

monitoring for registration communications emitting from a third device on the network;

completing said registration between said first device and said second device if no said registration communications emitting from said third device are detected; and

terminating said registration process without completing said registration between said first device and said second device if said registration communications from said third device are detected.

28. The process of claim 26, further comprising a step of generating a key at said second device.

29. The method of claim 26, further including a step of generating a pseudonym for a device.

30. The method of claim 26, wherein said identity information includes PIN number information.

31. The method of claim 26, wherein said first set of registration information does not include a plain-text device identifier.

32. The method of claim 26, wherein said second set of registration information does not include a plain-text device identifier.

33. A communications system with authentication, comprising:

a server;

a first network device in communication with said server;

a cryptographic key enabling authentic communications between said server and said first network device, wherein said cryptographic key is supported on said first network device and is formed through a registration process between said server and a second network device, wherein said registration process is launched at both said server and said second network device within a predetermined time interval of one another through an activation of each of a pair of registration triggers, each trigger coupled to one of said server and said second

network device, wherein said cryptographic key is transferred from said second network device to said first network device, thereby enabling said first network device to authenticate with said server.

34. The system of claim 33, wherein said registration process includes the use of PIN number information.

35. The system of claim 33, wherein at least one of said second network device and said server register without identifying the other in plain-text during said registration process.

36. The system of claim 33, wherein said registration process monitors for registration communications emitting from a third network device, whereby no detection of said registration communications results in completion of said registration process.

37. A method for establishing a mutually authenticated communications link, comprising:

establishing a one-way authenticated connection between a server and a client;

transmitting information between said server and said client through said connection to establish credentials that enable mutual authentication;

generating a shared secret at said client;

signaling to said server that said client knows said shared secret through said connection;

generating a shared secret at said server;

signaling to said client that said server knows said shared secret through said connection;

generating a key; and

establishing a two-way authenticated connection between said server and said client with said key.

38. The method of claim 37, wherein said one-way authentication connection is encrypted.

39. A system for establishing credentials for a mutual authentication between a server and a network device, comprising:

a first communications link formed between a server and a network device using a one-way authentication performed between said server and said network device;

a set of registration data exchanged between said server and said network device across said communications link to enable a mutual authentication between said server and said network device;

a cryptographic key formed at at least one of said server and said network device, thereby facilitating mutually authenticated communications between said server and said network device; and

a database supported on said network device storing said set of registration data and said cryptographic key.

40. The system of claim 39, wherein first communications link is encrypted.

41. A method for creating a communications link between two devices, comprising:

performing a one-way authentication between a pair of devices to establish a one-way authenticated communications link;

transmitting a set of registration information between said pair of devices across said one-way authenticated communications link;

establishing a set of credentials from said registration information; and

forming a two-way authenticated communications link using said set of credentials.

42. The system of claim 41, wherein said one-way authenticated communications link is encrypted.

43. The method of claim 41, wherein the forming step includes a step of generating a secret known by said pair of devices.

44. The method of claim 43, wherein said forming step includes a step of generating a key between said pair of devices.